AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on page 2, line 15 with the following amended paragraph:

FIG. 1A illustrates a representative example of a single security sensitive event formatted to~~ make if~~ make it readable by a human.

Please replace the paragraph beginning on page 3, line 15 with the following amended paragraph:

Fig. 1 is a block diagram of a system 100 for storing events to enhance intrusion detection. System 100 includes a plurality of computers 102, 106 and a network 101. Although system 100 includes computers 102, 106 for illustration purposes, different numbers of devices and network topologies may be included. Additionally, some~~ or the~~ of the data structures (to be described) as well as modules shown in system 100 can be implemented within a computing device, such as computer 106, or can be distributed within a computing system having more than one computing device. See the description of "Exemplary Computing System and Environment" below for specific examples and implementations of networks, computing systems, computing devices, and components that can be used to implement the described implementations, including computers 102, 106 and network 101.

Please replace the paragraph beginning on page 5, line 8 with the following amended paragraph:

The "header section" is a fixed length section of the event and has several fields, including: ~~and event~~ an event type (success/failure), event source, event category, event identification, date, time, user name and computer name (see FIG. 1A).

Please replace the paragraph beginning on page 5, line 11 with the following amended paragraph:

The "data section" is a variable length section of the event that is ~~stored in as~~ stored as set of strings. The number of strings present varies according to the "event identification" in the Event Header Section. For example, event 0x272(==626 decimal) contains six strings: foo, KUMARPDOM, KUMARPDOM\foo, Administrator, KUMARPDOM, (0x0, 0x237CE5) (see FIG. 1A).

Please replace the paragraph beginning on page 5, line 16 with the following amended paragraph:

The "event identification" (also referred ~~to event~~ to as event ID) identifies the type of event.

Please replace the paragraph beginning on page 5, line 20 with the following amended paragraph:

~~"Field (or event field)"~~ "Field" (or event field) means one of the strings in the data section of an event.

Please replace the paragraph beginning on page 6, line 5 with the following amended paragraph:

FIG. 1A illustrates a representative example of a single security sensitive event formatted to ~~make if~~ make it readable by a human, but stored in the event log.

Please replace the paragraph beginning on page 6, line 11 with the following amended paragraph:

In this example, the value "0x0272" is the event identification (the 0x prefix indicates the number is in hexadecimal format). Generally, the event identification follows the header text "MessageId=", regardless of the event type. Other formats could of course be used in other systems. In general, the event identification will ~~comprises~~ comprise code, text or an identification number, at a consistent or identifiable location within the event, that identify the particular type of event and corresponding security sensitive event.

Please replace the paragraph beginning on page 6, line 23 with the following amended paragraph:

In this example, each event descriptor comprises a descriptive phrase followed by a value. For example, the first descriptor in the above example contains the descriptive phrase "Target Account Name:", followed by a value. The values of the multiple descriptors can be in the form of numbers, text, or other information. They provide actual information about the event that corresponds to the event. Generally, the initial descriptive phrase describes the nature of the value that follows. For instance, if the descriptive phrase of the event descriptor is "logon ID," then the value that follows the descriptive phrase corresponds to the actual alphanumeric logon ID that was used in conjunction with the event corresponding to the event. As another example, if the descriptive phrase of the event descriptor is "target account" then the value that follows the descriptive phrase ~~indicate~~ indicates the actual alphanumeric target account number used in conjunction with the event corresponding to the event.